520.39632VX1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: S. FURUYA, et al

Serial No.: Not yet assigned

Filed: March 28, 2001

For: METHOD AND APPARATUS FOR SYMMETRIC-KEY ENCRYPTION

Group: Not yet assigned

Examiner: Not yet assigned

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §1.97 & 1.98

Assistant Commissioner
for Patents
Washington, D.C. 20231

March 28, 2001

Sir:

In the matter of the above-identified application, this Information Disclosure Statement is being submitted with the following citation as specified in 37 CFR §1.97(d).

> "A copy of any patent, publication or other information listed in an Information Disclosure Statement is not required to be provided if it was previously cited by or submitted to the Office in a prior application, provided that the prior application is properly identified in the statement and relied upon for an earlier filing date under 35 U.S.C. §120."

Applicant(s) are submitting herewith a copy of Form PTO-1449 which list documents cited in parent application(s) Serial No. 09/784,254, filed February 16, 2001.

It is respectfully requested that this information disclosure statement be considered by the Examiner.

Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to the deposit account of Antonelli, Terry, Stout & Kraus Deposit Account No. 01-2135 (520.39632VX1) please credit any excess fees to such deposit account.

Respectfully submitted,

Carl I. Brundidge
Registration No. 29,621
ANTONELLI, TERRY, STOUT & KRAUS, LLP

CIB/jdc
(703) 312-6600

FORM PTO-1449 U.S. Department of Commerce (Rev. 4/92) Patent and Trademark Office	ATTY. DOCKET NO.	SERIAL NO.
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Use several sheets if necessary)	520.39632VX1	Not yet assigned
	APPLICANT: S. FURUYA, et al	
	FILING DATE: March 28, 2001	GROUP: Not yet assigned

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT YES	ABSTRACT NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

		Advances in Cryptology-Crypto, etc.
		The Chain & Sum Primitive and its Applications to MACs and Stream Ciphers, M. Jakubowski et al, pp. 281-293, Advances in Cryptology Crypto '98 Kaisa Nyberg (Ed.).
		An Integrity Check Value Algorithm for Stream Ciphers, R. Taylor, pp. 40-48, Advances in Cryptology Crypto '93, D. Stinson (Ed.).
		Algorithm Types and Modes (189-401).
		UMAC: Fast and Secure Message Authentication, J. Black et al, pp. 216-269, Advances in Cryptology Crypto '99', M. Wiener (Ed.)
		MMH: Software Message Authentication in the Gbit/Second Rates, S. Halevi et al, 172-189, Fast Software Encryption, E. Biham (Ed.)
		Integrity-Aware PCBC Encryption Schemes, V. Gligor, 1-13, "The 1999 Security Protocols Workshop Pre-proceedings".
		Stream ciphers based on LFSRs pp. 203-369.
		Keying Hash Functions for Message Authentication Mihir Bellare et al, 1-328, Advances in Cryptology Crypto '96 Neal Koblitz (Ed.)

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.